CONTINUATION OF AN APPLICATION FOR A SEARCH WARRANT

I, Richard J. Trask, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a digital device—which is currently in law enforcement possession (the "Device"), as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since April 2011. As a Special Agent with the FBI, I have participated in, and conducted numerous investigations under the domestic terrorism, counterterrorism, and counterintelligence programs, to include espionage, terrorism, and domestic extremism investigations. I have participated in and executed search warrants to seize items of evidence from residences, telephone providers, and electronic devices, such as cell phones and computers. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of the following statutes have been committed by Jonathan Joshua Munafo ("MUNAFO"):

a. 18 U.S.C. § 875(c) (Interstate threatening communications);

b. 47 U.S.C. § 223(a)(1)(E) (Interstate harassing telephone calls);

c. 18 U.S.C. § 231(a)(3) (Civil disorder);

d. 18 U.S.C. § 111(a)(1) (Assaulting, resisting, or impeding certain officers);

e. 18 U.S.C. § 1512(c)(2) (Obstruction of an official proceeding);

f. 18 U.S.C. § 1752(a)(1) (Entering and remaining on restricted grounds with a dangerous weapon);

g. 18 U.S.C. § 1752(a)(2) (Disorderly and disruptive conduct in a restricted building or grounds with a dangerous weapon);

h. 18 U.S.C. § 1752(a)(4) (Act of physical violence against a person on restricted grounds with a dangerous weapon);

i. 40 U.S.C. § 5104(e)(2)(D) (Disorderly conduct in a Capitol building);

j. 40 U.S.C. § 5104(e)(2)(F) (Act of physical violence on the Capitol grounds).

There is also probable cause to search the Device, further described below and in Attachment A, for the things described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Samsung Tracfone, Model SM-S111DL (GP) wireless telephone, IMEI 352082504352669, that is, the "Device."

6. The Device is currently located at FBI Kalamazoo Resident Agency, 950 Trade Centre Way, Portage, Michigan 49002.

PROBABLE CAUSE

7. On January 5, 2021, MUNAFO placed numerous threatening phone calls to the emergency dispatcher in Calhoun County Michigan, from a rest stop in North Carolina. The following day (January 6, 2021) MUNAFO actively participated in the riots at the U.S. Capitol. He was charged by criminal complaint in the Western District of Michigan (1:21-mj-25) and the District of Columbia (1:21-mj-394). Grand juries in both districts subsequently returned felony indictments charging MUNAFO with the offenses listed in paragraph 4, above. (WDMI 1:21-cr-99; DDC 1:21-cr-330).

Munafo Threatens the Calhoun County Dispatcher

8. On January 8, 2021, I was informed by the Calhoun County Sheriff's office (CCSO) that an individual identifying himself as "Yankee Patriot" had made repeated threatening calls to the Calhoun County emergency dispatcher on January 5, 2021. The caller, later identified as MUNAFO, placed approximately 143 calls demanding to speak with a deputy sheriff or sergeant, tying up the emergency line for several hours.

9. I have listened to approximately 3 hours of MUNAFO's calls, which were recorded by CCSO. MUNAFO advised the 911 dispatcher that he knew where she lived, and recited accurate information about her mortgage and tax obligations. MUNAFO told the dispatcher he would maim her, kill her, and attack her family if she did not put a deputy or sergeant on the line. In one call he demanded, "[P]ut a fucking cop on the phone now you stupid bitch, or it's going to go way worse for your family!" In another he threatened, "[B]itch, I'm gonna cut your throat. I'm gonna make you eat your fucking nose. I'm gonna hurt you bad for this. It won't be today, it won't be tomorrow, it will be fucking soon though, you stupid cunt.

Insurrection Act, I'm coming to your door first and it's public knowledge, you stupid, stupid bitch!" MUNAFO was evidently aware he was breaking the law, stating, "each one of these calls are going to be like a charge, right? I'll never see a judge."

10. On or about January 6, 2021, CCSO's Detective Jonathan Pignataro determined through public records that the phone number making the threat calls was issued by "Bandwidth.com," an Internet phone service provider. A representative of Bandwidth.com advised Det. Pignataro that the number was resold by another Internet phone service provider, Textnow.com. Det. Pignataro served Textnow.com an emergency disclosure request followed by a search warrant. Textnow.com provided the subscriber's user name, Gmail address, and IP addresses used at the time of the threat calls, all of which were determined to belong to MUNAFO, as described below.

11. On January 6, 2021, Det. Pignataro also served a search warrant on Google LLC, for the Gmail account associated with the Textnow.com number. Google disclosed that the subscriber had provided username "adio8787," name "Johnny #5" and e-mail address adio8787@gmail.com. The subscriber also provided recovery email address jonathan.munafo@yahoo.com, and sign-in phone number (508) 418-9055.

12. Location information provided by Google in response to Det. Pignataro's search warrant establishes that MUNAFO was at a truck stop in Dunn, North Carolina when he placed the threat calls to the Calhoun County dispatcher on January 5, 2021.

13. In response to the Calhoun County search warrant, Google also provided MUNAFO's Internet search history for January 5, 2021, the day before the assault on the US Capitol. MUNAFO searched for information on "Calhoun Sheriff Michigan." Among other

searched terms disclosed by Google, MUNAFO also searched for "Freedom Plaza, Washington, DC," several firearms and military surplus stores, and "Gretchen Whitmer" on January 4 and 5, 2021.

Munafo Participates in the Capitol Riots

Background – The U.S. Capitol on January 6, 2021

14. The U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

15. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

16. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP.

Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

17. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

18. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

19. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

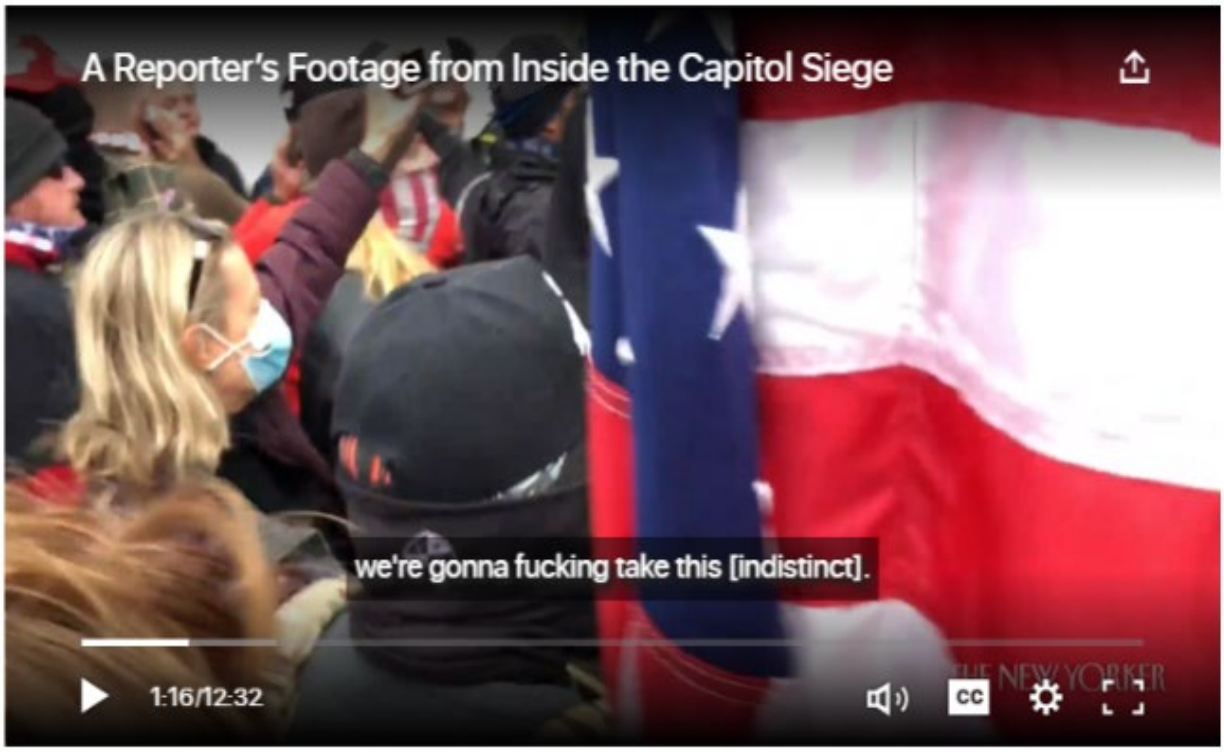
20. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

21. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

22. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

23. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

24. Shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, "We're gonna fucking take this," which your affiant believes was a reference to "taking" the U.S. Capitol.



25. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

26. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The

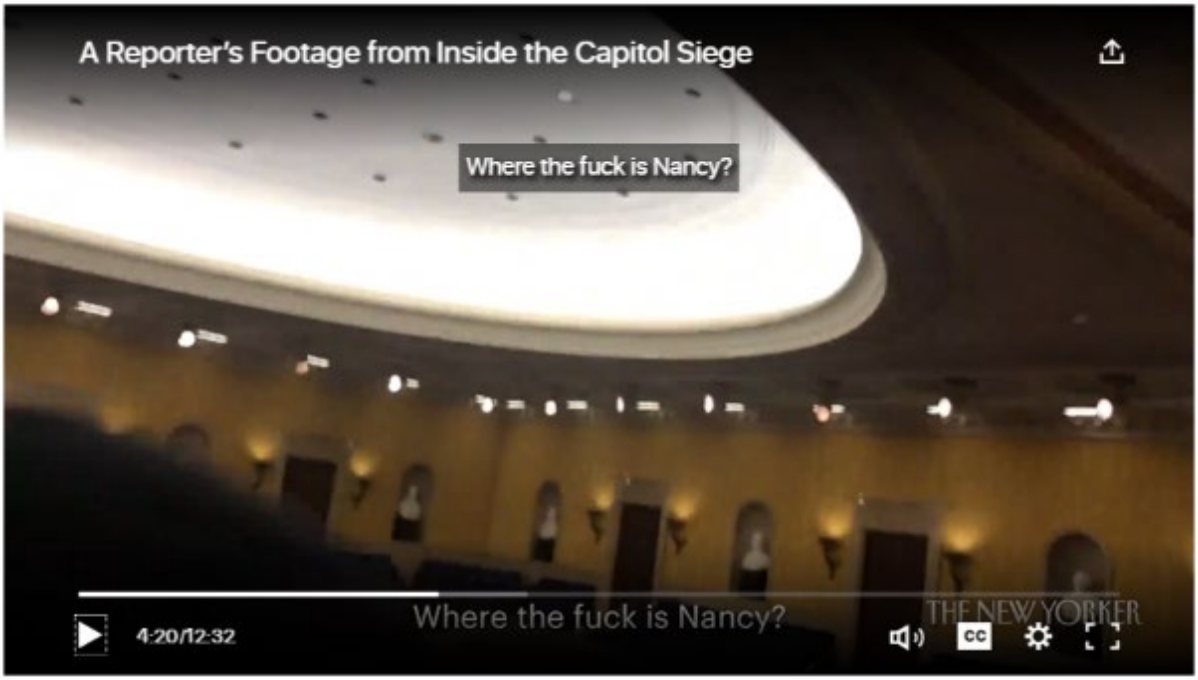
subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and Tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

27. Also at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

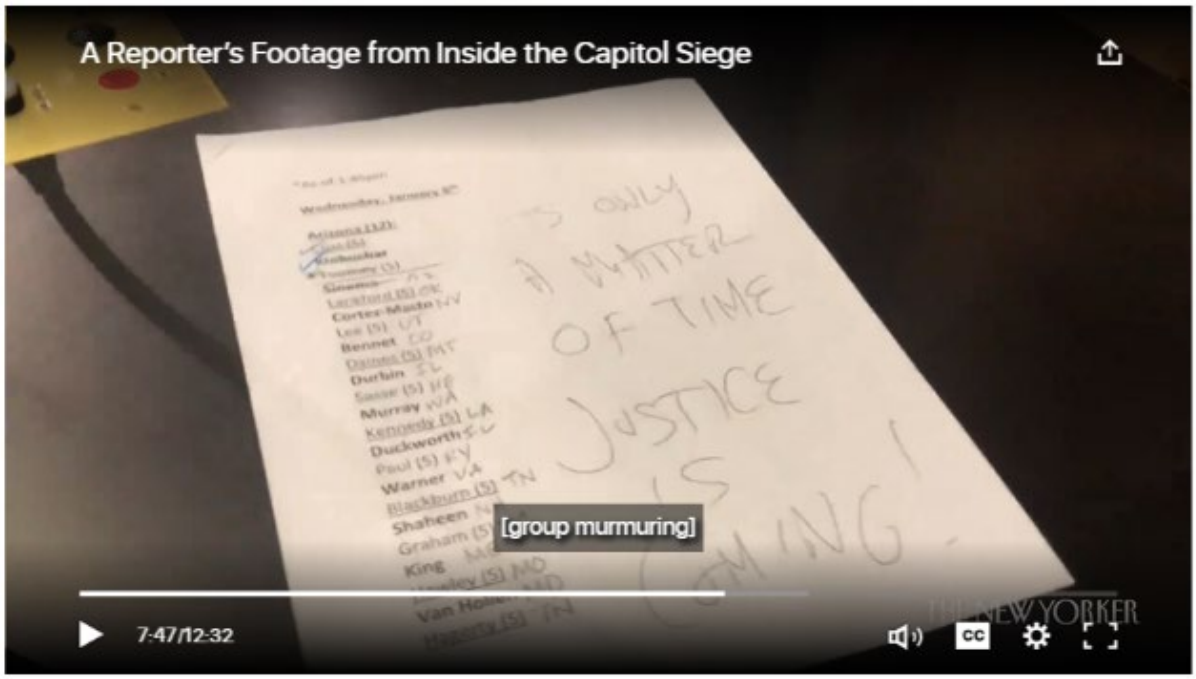
28. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

29. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, "Where are they?" as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word "they" is in reference to members of Congress.

30. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, "Where the fuck is Nancy?" Based upon other comments and the context, law enforcement believes that the "Nancy" being referenced was the Speaker of the House of Representatives, Nancy Pelosi.



31. An unknown subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated "A Matter of Time Justice is Coming."



32. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals were expected to be taken into custody.

33. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

34. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

35. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

36. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

37. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or

weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

38. Beginning around 8:00 p.m., the Senate resumed work on the Certification.

39. Beginning around 9:00 p.m., the House resumed work on the Certification.

40. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3 a.m. on January 7, 2021.

41. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

42. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

43. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of

themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

44. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:

[1]

[1] https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/

 [2]

 [3]

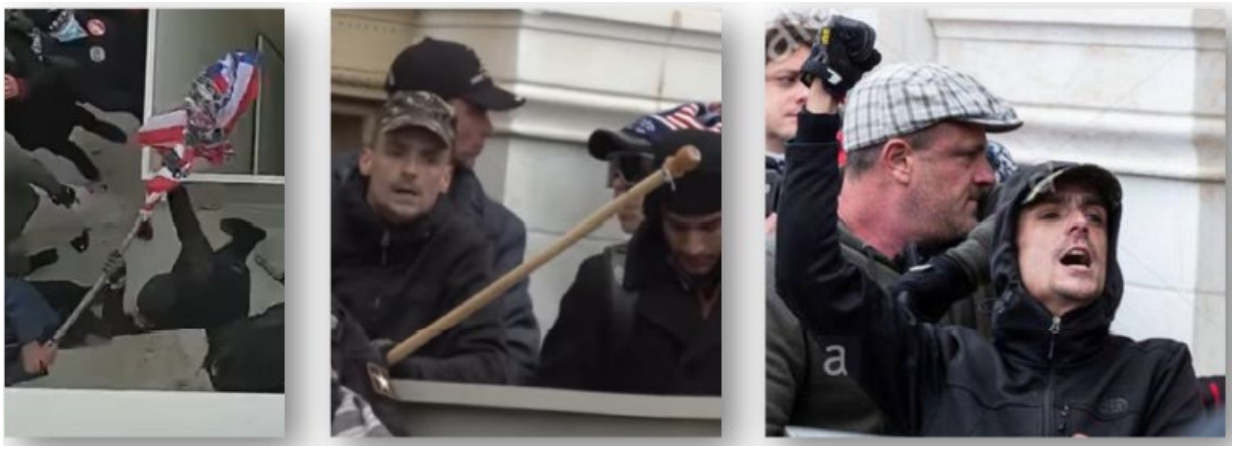
[2] https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1.

[3]https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e

Jonathan Munafo is Identified as a Riot and Assault Perpetrator:

45. Shortly after 2:00 p.m. on January 6, 2021, in the West Plaza of the Capitol, rioters attacked law enforcement and attempted to breach the police line. Not long after the initial surge, rioters broke through the police line and soon the West Plaza was overrun. The mob quickly turned violent. Rioters attacked USCP with fists, fire extinguishers, and "bike rack" style barricades.

46. At approximately 2:36 p.m., USCP fell back into the Capitol via the Arch/Tunnel Entrance to the Capitol building. For the next two and a half hours, until approximately 5:10 p.m., rioters continued attacking USCP in attempting to force themselves inside. During the battle, video captured an individual wearing a black hooded jacket (later identified as MUNAFO, as described below) striking a USCP officer twice in the head and body with a closed fist. The individual violently ripped the officer's riot shield out of his hands, and passed it back to other rioters behind him. Video footage also showed the individual using a flagpole to strike a window of the Capitol.



47. The FBI reviewed video footage of the riots, and assigned the subject the identifier "Suspect #170–AFO."[4] On March 18, 2021, the FBI released videos of assaults on

[4] The acronym "AFO" designates the suspect as being wanted for assault on a federal officer.

officers at the Capitol to seek the public's help in identifying suspects. The FBI identified Suspect #170–AFO as one of the top ten most wanted assault perpetrators from the Capitol riots, and posted three still photographs of him on its website.

48. On April 16, 2021, an FBI agent spoke with an individual (ID WITNESS 1), who identified Suspect #170–AFO as MUNAFO. ID WITNESS 1 said he had known MUNAFO for years, and said MUNAFO had told him he wanted to go to the "rally" in Washington D.C. on January 6, 2021. ID WITNESS 1 stated in sum and substance, "I believe it's him in the picture."

49. On April 17, 2021, an FBI agent spoke with an individual (ID WITNESS 2), who also identified Suspect #170–AFO as MUNAFO. ID WITNESS 2 said he/she had known MUNAFO for approximately twenty years, and had considered him a friend. After reviewing a photograph, ID WITNESS 2 stated in sum and substance, "I know it's him."

50. Law enforcement reviewed publicly available social media after the riots, and located a Twitter account in the name "Jonathan Munafo," with the handle "@the rightstuff87." The profile picture for the account appears to show the same individual identified as Suspect #170–AFO in the riot videos:

51. Law enforcement also reviewed an interview MUNAFO gave to a local TV station while attending a Trump rally in Manchester, New Hampshire in February, 2020. MUNAFO is identified as "John Munafo" of New York State in the video clip seen below. I have reviewed MUNAFO's New York State driver's license, and believe the individual pictured in the TV interview and license photo is Suspect #170–AFO.

52. On January 20, 2021, this Court issued a criminal complaint charging MUNAFO with making interstate threatening communications, in violation of 18 U.S.C. § 875(c). (WDMI 1:21-mj-25, R. 1, PageID.1.) On April 23, 2021, the District Court for the District of Columbia issued a criminal complaint charging MUNAFO with violations of 18 U.S.C. §§ 111(a)(1)(A); 1752(a)(1), (2) and (4); 1752(b)(1)(A); and 40 U.S.C. § 5104(e)(2). (DDC 1:21-mj-394, R. 1: Criminal Complaint.)

53. On April 23, 2021, MUNAFO was taken into federal custody, after being arrested by local authorities in the Middle District of Florida. (WDMI 1:21-mj-394, Warrant Returned Executed; DDC 1:21-mj-394, R. 5: Arrest Warrant Returned Executed.)

54. At the time of his arrest in Florida, MUNAFO was in possession of a Samsung Tracfone, Model SM-S111DL (GP) wireless telephone, IMEI 352082504352669, that is, the "Device." The Device was seized pursuant to arrest, and has been maintained in continuous law enforcement custody from that time, and is currently located at the FBI Kalamazoo Resident Agency, 950 Trade Centre Way, Portage, Michigan. Therefore, while the FBI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

55. On April 28, 2021, a grand jury in the District of Columbia returned an indictment charging MUNAFO with violations of 18 U.S.C. § 231(a)(3) (civil disorder); 18 U.S.C. §§ 111(a)(1) (assaulting, resisting or impeding certain officers); 1512(c)(2) (obstruction of an official proceeding); 1752(a)(1) and (b)(1)(A) (entering and remaining on restricted grounds with a dangerous weapon); 1752(a)(2) and (b)(1)(A) (disorderly and disruptive conduct in a restricted

building or grounds with a dangerous weapon); 1752(a)(4) and (b)(1)(A) (act of physical violence against property on restricted grounds with a dangerous weapon); 1752(a)(4) (act of physical violence against a person on restricted grounds); 641 (theft of government property); 40 U.S.C. §§ 5104(e)(2)(D) (disorderly conduct in a Capitol building); and 5104(e)(2)(F) (act of physical violence on the Capitol grounds).

56. On May 18, 2021, a grand jury in this district returned an indictment charging MUNAFO with two counts of making interstate threatening communications, in violation of 18 U.S.C. § 875(c), and one count of making interstate harassing telephone calls, in violation of 47 U.S.C. § 223(a)(1)(E). (WDMI 1:21-cr-99, R. 7: Indictment, PageID.17.)

TECHNICAL TERMS

57. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Wireless telephone" (or mobile telephone, or wireless telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books";

sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

b. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

58. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and personal digital assistant ("PDA"). In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offenses under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

59. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Device, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Device for at least the following reasons:

a. Individuals who engage in criminal activity use digital devices, like the Device, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or

viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

60. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information

related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This

data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to make threatening or harassing phone calls, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

61. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital

devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular

data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through

data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete.

Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

62. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital device, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital device may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword"

searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital device, the forensic examiners may examine as much of the contents of the digital device as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

63. Because forensic examiners will be conducting their search of the Device in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

64. I submit that this affidavit supports probable cause for a warrant to search the Device described in Attachment A and to seize the items described in Attachment B.